UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/863,932	05/22/2001	Brant Candelore	80398.P439	9990

7590 01/04/2005

BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP
Seventh Floor
12400 Wilshire Boulevard
Los Angeles, CA 90025-1026

EXAMINER	
TRUONG, LAN DAI T	

ART UNIT	PAPER NUMBER
2132	

DATE MAILED: 01/04/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/863,932	CANDELORE, BRANT	
	Examiner	Art Unit	
	Ian dai thi truong	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 03 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☐ Claim(s) 24 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☐ Claim(s) 24 is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on 22 May 2001 is/are: a)☐ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Specification

The number of provisional application shows on Oath is not correct. The correct number for provisional application is 60239317. Appropriate correction is required. 37CFR 1.76(d)

GB 12/27/04

Drawings

Some elements are in the drawing but they are not demonstrated in specification such as:

Figure 2, item: 240.

Figure 3, items: 320, 325, 330, 335, 340,345, 350, 355, 360.

Providing of detail information about those elements in specification is required.

Claim rejections-35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

Claims 1-2, 6-8,10, 12, 14, 19-20, 22 are rejected under 35 U.S.C. 102(e) as being anticipated by Tatu Ylonen. (U.S. 6,782,474), herein after referred to as Tatu Ylonen

1) In referring to claim 1:

1a) Limitation "accessing in a first device identification and at least one key corresponding to the device identification" is matched (column 2, lines 23-24; column3, lines 61-63;column 4, lines 45-46, column 6,13-19). Tatu Ylonen clearly taught that the device identifier is equivalent to "device identification" could be the cryptographic key itself what is "one key corresponding to the device identification". So, Marino's ideas meet the limitation of "accessing in a first device identification and at least one key corresponding to the device identification".

1b) Limitation "encoding data using the at least one key" is matched (column 8, lines 49-51, lines 60-64). Tatu Ylonen disclosed symmetric cryptographic keys use to cryptographically authenticate or encrypt any further messages what means "encoding data". The parties can directly use their secret key to encrypt any messages they send which is shared identical functionality with "encoding data using the at least one key".

1c) Limitation "transmitting a message from the first device to the second device, the messages comprising a header comprising the device identification and data field comprising the encoded data" is matched (column 1, lines 11-14; column 6, 26-34; figure 4, item 403, item 404; column 2, lines 5-20; column 4, lines 12-20). Tatu Ylonen disclosed method of data transmission between devices connected to the network. Also Tatu Ylonen taught about Encapsulating Security Payload (ESP) consists of header and followed encrypted data what is equivalent to "encoded data". The ESP header consists 32 bits Security Association Identifier which is equivalent to "device identification". Ideally, Tatu Yolonen's method meets the limitation of "transmitting a message from the first device to the second device, the messages comprising a header comprising the device identification and data field comprising the encoded data".

1d) Limitation "said second device using the device identification received in the header of message to determine the at least one key and decode the encoded data field received in the data field of the message using the determined at least one key" is matched (column 6, lines 5-11, lines 31-33; column 4 lines 45-59; column 8, lines 49-51, lines 60-64). Tatu Ylonen disclosed method using shared secret key what is equivalent device identification in the header of sending message to decrypt encryption message. So, ideally Tatu Ylonen's method meets limitation of "said second device using the device identification received in the header of message to determine the at least one key and decode the encoded data field received in the data field of the message using the determined at least one key".

2) In referring to claim 2:

Limitation "the method as set forth in claim 1, wherein the device identification is selected from the group consisting of a unique device identification of the first device, a unique device identification of the second device, a device address of the first device, and second device" is matched (column 6, lines 1-5). Tatu Ylonen disclosed each network device have a device identifier which is equivalent to "a unique device identification" could be printed on a sticker and attached to the bottom of the device.

3) In referring to claim 6:

Limitation "the method as set forth in claim 1, wherein the at least one key for encoding is selected from the group consisting of hashing and signing a message and encrypting a message" is matched (column 8, lines 49-51, 60-64). Tatu Ylonen disclosed using shared secret key to encrypt message, what meets limitation of "the at least one key for encoding is selected from the group consisting of hashing and signing a message and encrypting a message".

4) In referring to claim 7:

Limitation "the method as set forth in claim 1, wherein the device identification is selected from the group consisting of a unique network identification that is a mandatory part of a standard communication protocol, a unique device address, a unique device identification and a Media Access Control (MAC) address" is matched (column 8, lines 1-5). Tatu Ylonen disclosed device identifier is equivalent to "unique device identification" could be printed on a sticker and attached to the bottom of the device, what meets the limitation of "wherein the device identification is selected from the group consisting of a unique network identification that is a mandatory part of a unique device identification".

5) In referring to claim 8:

A communication device comprising:

5a) Limitation "a non-volatile storage medium for storing information for at least one key corresponding to a device identification of a communication device" is matched (column 9, lines 35-45). Tatu Ylonen disclosed a non-volatile memory is "a non-volatile storage medium" to store device identifier that mean "key corresponding to a device identification of a communication device". So, Tatu Ylonen's ideas meet limitation of "a non-volatile storage medium for storing information for at least one key corresponding to a device identification of a communication device".

5b) Limitation "a first logic to encode data using the at least one key and decode encoded data using the at least one key" is matched (column 8, lines 49-52, 60-64). Tatu Ylonen disclosed using shared secret key to encrypt the message then decrypt the encrypted message.

What meets the limitation of "using the at least one key and decode encoded data using the at least one key".

5c) Limitation "an input/output to communicate encoded data in a message, the message including the device identification and the encoded data" is matched (column 5, lines 64-67;column 9, lines 35-67; column 10, lines 14-18, figure 7, item708, 707). Tatu Ylonen disclosed physical network interface include keyboard is input and display screen is output, what meets the limitation of "an input/output to communicate encoded data in a message".

6) In referring to claim 10:

Limitation "the device as set forth in claim 8, wherein the information comprised the at least one key and corresponding device identification" is matched (column 2, lines 23-24; column3, lines 61-63;column 4, lines 45-46, column 6,13-19). Tatu Ylonen clearly taught that the device identifier is equivalent to "device identification" could be the cryptographic key itself what is shared identical functionality with "one key corresponding to the device identification". So, Marino's ideas meet the limitation of "the device as set forth in claim 8, wherein the information comprised the at least one key and corresponding device identification".

7) In referring to claim 12:

Limitation "the device as set forth in claim 8, wherein the device is selected from the group consisting of a device to connect to a cable network, a direct broadcast satellite (BDS) device, a phone device, an internet device, a broadcast device and a set top box" is matched (column 1,lines 15-21, 24-27). Tatu Ylonen disclosed network devices such as network camera which is equivalent to a device to connect to a cable network, router is equivalent to an Internet device, and print servers and network printer which is equivalent to a device to connect to cable

network and/or set top box. So, Tatu Ylonen's ideas meet limitation of "wherein the device is selected from the group consisting of a device to connect to a cable network, a direct broadcast satellite (BDS) device, a phone device, an Internet device, a broadcast device and a set top box."

8) In referring to claim 19:

Limitation "the device as set forth in claim 8, wherein the message is selected from the group consisting of hashing and signing a message and encryption" is matched (column 8, lines 49-52). Tatu Ylonen disclosed using shared secret key to encrypt message, what meets limitation of "wherein the message is selected from the group consisting of hashing and signing a message and encryption".

9) In referring to claim 20: a system comprises

At least one first device, said first device comprising

- Limitation "A non-volatile storage medium for storing information for at least one key corresponding to a device identification of first device" is matched (column 9, lines 35-49). Tatu Ylonen disclosed a non-volatile memory to store device identifier, what meets the limitation of "a non-volatile storage medium for storing information for at least one key corresponding to a device identification of a communication device".
- Limitation "A first logic to encode data using the at least one key and decode encoded data using the at least one key" is matched (column 8, lines 49-52, 60-64). Tatu Ylonen disclosed using shared secret key is device identification to encrypt the message then decrypt the encrypted message. So, Tatu Ylonen's ideas

meet the limitation of "using the at least one key and decode encoded data using the at least one key".

- Limitation "An input/output to communicate encoded data in a message, the message including the device identification of the first device and the encoded data" is matched (column 5, lines 64-67;column 9, lines 47-67; column 10, lines 14-18). Tatu Ylonen disclosed physical network interface, keypad is input and display screen is output, what meets the limitation of "an input/output to communicate encoded data in a message".
- "At least on second device coupled to the first device through the communication medium, the second device comprising:
- Limitation "A non-volatile storage medium for storing information for at least one key corresponding to a device identification of the first device" is matched (column 9, lines 35-49). Tatu Ylonen disclosed a non-volatile memory to store device identifier, what meets the limitation of "a non-volatile storage medium for storing information for at least one key corresponding to a device identification of a communication device".
- Limitation "A second logic to encode data using the at least one key and decode encoded data using the at least one key" is matched (column 8, lines 49-52, 60-64). Tatu Ylonen disclosed using shared secret key what is device identification to encrypt the message then decrypt the encrypted message. What meets the limitation of "using the at least one key and decode encoded data using the at least one key".

Limitation " An input/output to communicate encoded data in a message, the messages including the device identification of the first device and the encoded data" is matched (column 5, lines 64-67;column 9, lines 35-67; column 10, lines 14-18; figure 3, item 403, item 404). Tatu Ylonen disclosed physical network interface, keypad is input and display screen is output, what meets the limitation of "an input/output to communicate encoded data in a message".

10) In referring to claim 22:

Limitation " the system as set forth in claim 20, wherein the information comprises the at least one key and corresponding device identification" is matched (column 4, lines 45-47, 54-59, column 6, lines 1-5,13-19, column3, lines 56-63). Tatu Ylonen clearly taught that the device identifier could be the cryptographic key itself, what meets the limitation of "at least one key and corresponding device identification"

Claim rejections-35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or descry bed as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.\

11) Claim 3 is rejected under 35 U.S.C. 103(a) as being unpatentable over Tatu Ylonen. (U.S. 6,782,474), as applied to claim 1 above, and further in view of Campbell (U.S. 4,605,820)

In referring to claim 3:

Limitation "the method as set forth in claim 1, wherein the at least one key is generated using the device identification and a plurality of generation keys" is matched (column2, lines 38-47; column 3, lines 45-67; column 4, lines 1-6, 41-44).

Tatu Ylonen disclosed:

- Accessing in a first device identification and at least one key corresponding to the device identification.
- Encoding data using the at least one key.
- Transmitting a message from the first device to the second device, the messages comprising a header comprising the device identification and data field comprising the encoded data.
- Said second device using the device identification received in the header of message to determine the at least one key and decode the encoded data field received in the data field of the message using the determined at least one key

But Tatu Ylonen failed to disclose "wherein the at least one key is generated using the device identification and a plurality of generation keys." However, Campbell disclosed key management system for on-line communication. Campbell taught how to generate the 50 values what are equivalent to the "generation keys" of primary key table by using one first initial double-length key what is equivalent to "device identification" proceeds with elements in the modifier table. In Campbel's method, After 10 entries of the first column of primary key table have been generated by using the first initial double-length key, the next step is generation of 10 entries for the second column of primary key table by using the first entry of the first column as the input value proceeds with the elements

in the modifier table. For the third column, using the first entry of second column to generate 10 entries in third column. This procedure continues until all row of all five columns have been generated. It would have been obvious to a person of ordinary skill in the art at the time the invention was make of "wherein the at least one key is generated using the device identification and a plurality of generation keys" because first entries of each column what have been used as the input values to generate next 10 entries in the next column are "generation keys", the hex-digits of each input entry what is used for generation 10 entries of next column is also device identification. The motivation would have been obvious because on of ordinary skill in the art would have been motivated to improve security key system for on-line communication and there is no need for large storage of keys at the central host.

12) Claim 4 is rejected under 35 U.S.C. 103(a) as being unpatentable over Tatu Ylonen. (U.S. 6,782,474), as applied to claim 1 above, and further in view of Campbell (U.S. 4,605,820)

In referring to claim 4:

Limitation " the method as set forth in claim 3, further comprising generating the at least one key using a multistage process wherein a different generation key of the plurality of generation key is used at each stage to operate with the output of a prior stage, a first stage having as input the device identification, and the a last stage outputting a key of the at least one key" is matched (column 3, 30-67; column 4, lines 1-5).

Tatu Ylonen disclosed:

- Accessing in a first device identification and at least one key corresponding to the device identification.

- Encoding data using the at least one key.
- Transmitting a message from the first device to the second device, the messages comprising a header comprising the device identification and data field comprising the encoded data.
- Said second device using the device identification received in the header of message to determine the at least one key and decode the encoded data field received in the data field of the message using the determined at least one key

But Tatu Ylonen failed to disclose "further comprising generating the at least one key using a multistage process wherein a different generation key of the plurality of generation key is used at each stage to operate with the output of a prior stage, a first stage having as input the device identification, and the a last stage outputting a key of the at least one key." However, Campbell disclosed key management system for on-line communication. Campbell taught using the first and second 16 hex digits of input value proceeds with elements in modifier table, and method of exclusive-OR 2 times what is " multistage" to produce 32 hex digits output value what is equivalent generation key in primary key table. It would have been obvious to a person of ordinary skill in the art at the time the invention was make of "one key using a multistage process wherein a different generation key of the plurality of generation key is used at each stage to operate with the output of a prior stage, a first stage having as input the device identification, and the a last stage outputting a key of the at least one key" because the time of exclusive-or performances is "Multistage" and input value for first time exclusive-or is device identification, and the key is produced from the second exclusive-or by using output of

first time exclusive-or as input value. So, ideally Campbell's method meets limitation of "further comprising generating the at least one key using a multistage process wherein a different generation key of the plurality of generation key is used at each stage to operate with the output of a prior stage, a first stage having as input the device identification, and the a last stage outputting a key of the at least one key." The motivation would have been obvious because on of ordinary skill in the art would have been motivated to generate key from generation key.

13) Claim 5 is rejected under 35 U.S.C. 103(a) as being unpatentable over Tatu Ylonen. (U.S. 6,782,474), as applied to claim 1 above, and further in view of Campbell (U.S. 4,605,820)

In referring to claim 5:

Limitation "the method as set forth in claim 4, wherein each stage is selected from the group consisting of a cipher function, a Exclusive OR function, a mathematical function, a logic function, a function that complies with the Advance Encryption Standard (AES), a function that complies with the Data Encryption Standard (DES) and functions that comply with determined encryption standards" is matched (column 3, lines 30- 45).

Tatu Ylonen disclosed:

- Accessing in a first device identification and at least one key corresponding to the device identification.
- Encoding data using the at least one key.
- Transmitting a message from the first device to the second device, the messages comprising a header comprising the device identification and data field comprising the encoded data.

- Said second device using the device identification received in the header of message to determine the at least one key and decode the encoded data field received in the data field of the message using the determined at least one key

But Tatu Ylonen failed to teach "wherein each stage is selected from the group consisting of a cipher function, a Exclusive OR function, a mathematical function, a logic function, a function that complies with the Advance Encryption Standard (AES), a function that complies with the Data Encryption Standard (DES) and functions that comply with determined encryption standards." However, Campbel disclose the keys of primary key table are produced from the exclusive-OR of the result output values of the previous exclusive-OR. It would have been obvious to a person of ordinary skill in the art at the time the invention was make of "wherein each stage is selected from the group consisting of a cipher function, a Exclusive OR function, a mathematical function, a logic function, a function that complies with the Advance Encryption Standard (AES), a function that complies with the Data Encryption Standard (DES) and functions that comply with determined encryption standards" because Campbel's method using Exclusive OR function to generate the key. The motivation would have been obvious because on of ordinary skill in the art would have been motivated to generate key from generation key.

14) Claim 9 is rejected under 35 U.S.C. 103(a) as being unpatentable over Tatu Ylonen. (U.S. 6,782,474), as applied to claim 8 above, and further in view of Marino (U.S. 6,026,165)

In referring to claim 9:

Limitation "the device as set forth in claim 8, wherein a first communication device communicates with a second communication device and the device identification corresponds to the first communication device" is matched (column 7, lines 52-67; column 8, lines 1-6).

Tatu Ylonen disclosed

- A non-volatile storage medium for storing information for at least one key corresponding to a device identification of a communication device.
- A first logic to encode data using the at least one key and decode encoded data using the at least one key.
- An input/output to communicate encoded data in a message, the message including the device identification and the encoded data

But Tatu Ylonen failed to teach about "wherein a first communication device communicates with a second communication device and the device identification corresponds to the first communication device." However, Marino disclosed transmitters need to register their identifications to receiver then all record of device identification is stored in EEPROM in receiver. When receiver receives encrypted data from the transmitter, it is going to looking for match transmitter identification, and when receiver finds the proper record, it is going to use transmitter identification for message encrypting. It would have been obvious to a person of ordinary skill in the art at the time the invention was make of "wherein a first communication device communicates with a second communication device and the device identification corresponds to the first communication device" because transmitters which is equivalent to "first communication device", receiver which is equivalent to "second communication device"

and transmitter identification which is equivalent to "the device identification corresponding to the first communication device". So, Marino's ideas meet limitation of "wherein the device comprised a service provider that communicates data with a second device, the device identification corresponding to the second device." The motivation would have been obvious because on of ordinary skill in the art would have been motivated to allow the user to easily and readily register any transmitting device's randomly generated encryption key (device identification) with receiver to ensure the maximum security of the system.

15) Claim 11 is rejected under 35 U.S.C. 103(a) as being unpatentable over Tatu Ylonen. (U.S. 6,782,474), as applied to claim 8 above, and further in view of Campbell (U.S. 4,605,820)

In referring to claim 11:

Limitation "the device as set forth in claim 8, wherein the information comprises generation keys, the generation keys used with the device identification to generate the at least one key" is matched (column2, lines 38-47; column 3, lines 45-67; column 4, lines 1-6, 41-44).

Tatu Ylonen disclosed

- A non-volatile storage medium for storing information for at least one key corresponding to a device identification of a communication device.
- A first logic to encode data using the at least one key and decode encoded data using the at least one key.
- An input/output to communicate encoded data in a message, the message including the device identification and the encoded data.

But he failed to disclose "wherein the information comprises generation keys, the generation keys used with the device identification to generate the at least one key." However,

Campbell disclosed key management system for on-line communication. Campbell taught how to generate the 50 values what are equivalent to the "generation keys" of primary key table by using one first initial double-length key what is equivalent to "device identification" proceeds with elements in the modifier table. In Campbel's method, After 10 entries of the first column of primary key table have been generated by using the first initial double-length key, the next step is generation 10 entries for the second column of primary key table by using the every first entry of the first column as the input value proceeds with the elements in the modifier table. For the third column, using the every first entry of second column to generate 10 entries in third column. This procedure continues until all row of all five columns have been generated. It would have been obvious to a person of ordinary skill in the art at the time the invention was make of "wherein the information comprises generation keys, the generation keys used with the device identification to generate the at least one key." because first entries of each column what have been used as the input values to generate next 10 entries in the next column are "generation keys", the hex-digits of each input entry what is used for generation 10 entries of next column is also device identification. So, Ideally Campbell's method meets limitation of "wherein the information comprises generation keys, the generation keys used with the device identification to generate the at least one key." The motivation would have been obvious because on of ordinary skill in the art would have been motivated to improve security key system for on-line communication and there is no need for large storage of keys at the central host.

16) Claim 13, 14 are rejected under 35 U.S.C. 103(a) as being unpatentable over Tatu Ylonen. (U.S. 6,782,474), as applied to claim 8 above, and further in view of Marino (U.S. 6,026,165)

15a) In referring to claim 13:

Limitation "the device as set forth in claim 8, wherein the device comprised a service provider that communicates data with a second device, the device identification corresponding to the second device" is matched (column 7, lines 52-67; column 8, lines 1-6).

Tatu Ylonen disclosed

- A non-volatile storage medium for storing information for at least one key corresponding to a device identification of a communication device.
- A first logic to encode data using the at least one key and decode encoded data using the at least one key.
- An input/output to communicate encoded data in a message, the message including the device identification and the encoded data.

But he failed to teach "wherein the device comprised a service provider that communicates data with a second device, the device identification corresponding to the second device." However, Marino disclosed transmitters need to register their identifications to receiver then all record of device identification is stored in EEPROM in receiver. When receiver receives encrypted data from the transmitter, it is going to looking for match transmitter identification, and when receiver finds the proper record, it is going to use transmitter identification for message encrypting. It would have been obvious to a person of ordinary skill in the art at the time the invention was make of "wherein the device comprised a service provider that communicates data with a second device, the device identification corresponding to the second device" because transmitters which is equivalent to "second device", receiver which is equivalent to "service provider" and transmitter identification which is equivalent to "the device

identification corresponding to the second device". The motivation would have been obvious because on of ordinary skill in the art would have been motivated to allow the user to easily and readily register any transmitting device's randomly generated encryption key (device identification) with receiver to ensure the maximum security of the system.

17 b) In referring to claim 14:

Limitation "the device as set forth in claim 13, wherein the device is a cable provider head end, a DBS uplink, a digital subscriber line (DSL) center, website and the second device is a set tip box" is matched (column 1, lines 24-29,column 4, lines 9-27). Tatu Ylonen disclosed a network device such as router, network camera, and telecommunications adapters that means providers must be cable provider, digital subscriber line provider, website. So, Tatu Ylonen's ideas meet the limitation of "device is a cable provider head end, a DBS uplink, a digital subscriber line (DSL) center, website".

18) Claim 15 is rejected under 35 U.S.C. 103(a) as being unpatentable over Tatu Ylonen. (U.S. 6,782,474), as applied to claim 8 above, and further in view of Marino (U.S. 6,026,165)

In referring to claim 15:

Limitation "the device as set forth in claim 8, wherein the non-volatile storage medium is selected from the group consisting of FLASH memory, static random access memory (SRAM), hard-disk media, memory stick, battery-backed RAM, fused, non-volatile removable media and optical media" is matched (column 5, lines 44-47; column 7, line 3-12). Tatu Ylonen disclosed

- A non-volatile storage medium for storing information for at least one key corresponding to a device identification of a communication device.

- A first logic to encode data using the at least one key and decode encoded data using the at least one key.
- An input/output to communicate encoded data in a message, the message including the device identification and the encoded data.

But he failed to teach for "wherein the non-volatile storage medium is selected from the group consisting of FLASH memory, static random access memory (SRAM), hard-disk media, memory stick, battery-backed RAM, fused, non-volatile removable media and optical media." However, Marino disclosed using non-volatile memory to store encrypting data, and the encryption key and sequence number. Marino also taught that his non-volatile memory is EEPROM memory. It would have been obvious to a person of ordinary skill in the art at the time the invention was make of "the non-volatile storage medium is selected from the group consisting of FLASH memory, static random access memory (SRAM), hard-disk media, memory stick, battery-backed RAM, fused, non-volatile removable media and optical media" because EEPROM is equivalent to FLASH memory or hard-disk media.. The motivation would have been obvious because on of ordinary skill in the art would have been motivated to use the FLASH memory to erase and reprogram.

19) Claim 16 is rejected under 35 U.S.C. 103(a) as being unpatentable over Tatu Ylonen. (U.S. 6,782,474), as applied to claim11 above, and further in view of Campbell (U.S. 4,605,820)

In referring to claim 16:

Limitation " the device as set forth in claim 11, further comprising a second logic, the second logic using the generation keys and the device identification to generate the at least one key" is matched (column2, lines 38-47; column 3, lines 45-67; column 4, lines 1-6, 41-44).

Tatu Ylonen disclosed

- A non-volatile storage medium for storing information for at least one key corresponding to a device identification of a communication device.
- A first logic to encode data using the at least one key and decode encoded data using the at least one key.
- An input/output to communicate encoded data in a message, the message including the device identification and the encoded data.

But he failed to teach this limitation: "further comprising a second logic, the second logic using the generation keys and the device identification to generate the at least one key." However, Campbell disclosed key management system for on-line communication. Campbell taught how to generate the 50 values what are equivalent to the "generation keys" of primary key table by using one first initial double-length key what is equivalent to "device identification" proceeds with elements in the modifier table. In Campbel's method, After 10 entries of the first column of primary key table have been generated by using the first initial double-length key, the next step is generation 10 entries for the second column of primary key table by using the every first entry of the first column as the input value proceeds with the elements in the modifier table. For the third column, using the every first entry of second column to generate 10 entries in third column. This procedure continues until all row of all five columns have been generated. It would have

been obvious to a person of ordinary skill in the art at the time the invention was make of "further comprising a second logic, the second logic using the generation keys and the device identification to generate the at least one key" because first entries of each column what have been used as the input values to generate next 10 entries in the next column are "generation keys", the hex digits of each input entry what is used for generation 10 entries of next is also device identification. So, Ideally Campbell's method meets limitation of "further comprising a second logic, the second logic using the generation keys and the device identification to generate the at least one key." The motivation would have been obvious because on of ordinary skill in the art would have been motivated to improve security key system for on-line communication and there is no need for large storage of keys at the central host.

20) Claim 17 is rejected under 35 U.S.C. 103(a) as being unpatentable over Tatu Ylonen. (U.S. 6,782,474), as applied to claim 1 above, and further in view of Campbell (U.S. 4,605,820)

In referring to claim 17:

"a first sub-logic having as input the device identification and a first generation key of the generation keys, said first sub-logic generating a first output

a second sub-logic having as input the first output and a second generation key of the generation keys, said second sub-logic generating a second output

a third sub-logic having as input the second output and a third generation key of the plurality of generation keys, said third sub-logic generation key as output" is matched (column 3, lines 30-67, column 4, lines 1-5).

Tatu Ylonen disclosed:

- A non-volatile storage medium for storing information for at least one key corresponding to a device identification of a communication device.
- A first logic to encode data using the at least one key and decode encoded data using the at least one key.
- An input/output to communicate encoded data in a message, the message including the device identification and the encoded data.

But Tatu Ylonen failed to teach about "a first sub-logic having as input the device identification and a first generation key of the generation keys, said first sub-logic generating a first output. A second sub-logic having as input the first output and a second generation key of the generation keys, said second sub-logic generating a second output. A third sub-logic having as input the second output and a third generation key of the plurality of generation keys, said third sub-logic generation key as output." However, ~~Campbell~~ Campbell disclosed key management system for on-line communication. Campbell taught using one first initial double-length key what is equivalent to "device identification" proceeds with elements in the modifier table to generate 10 entries of the first column of primary key table. After all row of the first column have been generated by using the first initial double-length key, the next step is generation 10 entries for the second column of primary key table by using the every first entry of the first column as the input value proceeds with the elements in the modifier table. For the third column, using the every first entry of second column to generate 10 entries in third column. This procedure continues until all row of all five columns have been generated. It would have been obvious to a person of ordinary skill in the art at the time the invention was make of

"a first sub-logic having as input the device identification and a first generation key of the generation keys, said first sub-logic generating a first output. A second sub-logic having as input the first output and a second generation key of the generation keys, said second sub-logic generating a second output. A third sub-logic having as input the second output and a third generation key of the plurality of generation keys, said third sub-logic generation key as output" because first initial entry of first column is "device Identification" what is used to generate the output values what are " first sub-logic generating first output" for the first column, then first output value of first column is use as the input value to generate output values are keys in next column. Then the procedure continues until get output values are keys what are used for PIN encryption. The motivation would have been obvious because on of ordinary skill in the art would have been motivated to improve security key system for on-line communication and there is no need for large storage of keys at the central host.

21) Claim 18 is rejected under 35 U.S.C. 103(a) as being unpatentable over Tatu Ylonen. (U.S. 6,782,474), as applied to claim 8 above, and further in view of Campbell (U.S. 4,605,820)

In referring to claim 18:

Limitation "the device as set forth in claim 17, wherein the first sub-logic, second sub-logic and third sub-logic are functions selected from the group consisting of logic functions, combinatorial functions and cipher functions" is matched (column 3, lines 30-45).

Tatu Ylonen disclosed:

- A non-volatile storage medium for storing information for at least one key corresponding to a device identification of a communication device.
- A first logic to encode data using the at least one key and decode encoded data using the at least one key.
- An input/output to communicate encoded data in a message, the message including the device identification and the encoded data

But Tatu Ylonen didn't teach about "wherein the first sub-logic, second sub-logic and third sub-logic are functions selected from the group consisting of logic functions, combinatorial functions and cipher functions." However, Campbell disclosed the keys of primary key table are produced from the second exclusive-OR by using output value of first exclusive-OR as the input value. It would have been obvious to a person of ordinary skill in the art at the time the invention was make of "wherein the first sub-logic, second sub-logic and third sub-logic are functions selected from the group consisting of logic functions, combinatorial functions and cipher functions" because Campbel's method uses Exclusive OR function which is equivalent to "logic function" to generate the key. The motivation would have been obvious because on of ordinary skill in the art would have been motivated to improve security key system for on-line communication.

22) Claim 21 is rejected under 35 U.S.C. 103(a) as being unpatentable over Tatu Ylonen. (U.S. 6,782,474), as applied to claim 8 above, and further in view of Marino (U.S. 6,026,165)

In referring to claim 21:

Limitation "the system set forth in claim 20, wherein the second device communicates with a plurality of first devices, the non-volatile storage medium of the second device storing

i nformation for at least one key for each first device" is matched (column 7, lines 52-67; column 8, lines 1-6).

Tatu Ylonen disclosed:

- A non-volatile storage medium for storing information for at least one key corresponding to a device identification of first device
- A first logic to encode data using the at least one key and decode encoded data using the at least one key
- An input/output to communicate encoded data in a message, the message including the device identification of the first device and the encoded data

But he failed to teach about "wherein the second device communicates with a plurality of first devices, the non-volatile storage medium of the second device storing information for at least one key for each first device." However, Marino disclosed transmitters need to register their identifications to receiver then all record of device identification is stored in EEPROM in receiver. When receiver receives encrypted data from the transmitter, it is going to looking for match transmitter identification, and when receiver finds the proper record, it is going to use transmitter identification for message encrypting. It would have been obvious to a person of ordinary skill in the art at the time the invention was make of "wherein the second device communicates with a plurality of first devices, the non-volatile storage medium of the second device storing information for at least one key for each first device" because transmitters which is equivalent to "first devices", receiver which is equivalent to "second device" and EEPROM is non-volatile storage medium of the second device to store the identification of first device. So, Marino's ideas meet limitation of "wherein the device comprised a service provider

that communicates data with a second device, the device identification corresponding to the second device." The motivation would have been obvious because on of ordinary skill in the art would have been motivated to allow the user to easily and readily register any transmitting device's randomly generated encryption key (device identification) with receiver to ensure the maximum security of the system.

23) Claim 23 is rejected under 35 U.S.C. 103(a) as being unpatentable over Tatu Ylonen. (U.S. 6,782,474), as applied to claim 20 above, and further in view of Campbell (U.S. 4,605,820)

In referring to claim 23:

Limitation " the device as set forth in claim 20, wherein the information comprises generation keys, the generation keys used with the device identification to generate the at least on key" is matched (column2, lines 38-47; column 3, lines 45-67; column 4, lines 1-6, 41-44).

Tatu Ylonen disclosed

-At least one first device, said first device comprising:

- A non-volatile storage medium for storing information for at least one key corresponding to a device identification of first device
- A first logic to encode data using the at least one key and decode encoded data using the at least one key
- An input/output to communicate encoded data in a message, the message including the device identification of the first device and the encoded data

-At least on second device coupled to the first device through the communication medium, the second device comprising:

- A non-volatile storage medium for storing information for at least one key corresponding to a device identification of the first device.
- A second logic to encode data using the at least one key and decode encoded data using the at least one key.
- An input/output to communicate encoded data in a message, the messages including the device identification of the first device and the encoded data.

But he failed to disclose "wherein the information comprises generation keys, the generation keys used with the device identification to generate the at least one key." However, Campbell disclosed key management system for on-line communication. Campbell taught how to generate the 50 values what are equivalent to the "generation keys" of primary key table by using one first initial double-length key what is equivalent to "device identification" proceeds with elements in the modifier table. In Campbel's method, After 10 entries of the first column of primary key table have been generated by using the first initial double-length key, the next step is generation 10 entries for the second column of primary key table by using the every first entry of the first column as the input value proceeds with the elements in the modifier table. For the third column, using the every first entry of second column to generate 10 entries in third column. This procedure continues until all row of all five columns have been generated. It would have been obvious to a person of ordinary skill in the art at the time the invention was make of "wherein the information comprises generation keys, the generation keys used with the device identification to generate the at least one key." because first entries of each column what have been used as the input values to generate next 10 entries in the next column are "generation keys", the hex digits of each input entry what is used for generation 10 entries of

next is also device identification. So, Ideally Campbell's method meets limitation of "wherein the information comprises generation keys, the generation keys used with the device identification to generate the at least one key." The motivation would have been obvious because on of ordinary skill in the art would have been motivated to improve security key system for on-line communication and there is no need for large storage of keys at the central host.

24) Claim 24 is rejected under 35 U.S.C. 103(a) as being unpatentable over Tatu Ylonen. (U.S. 6,782,474), as applied to claim 20 above, and further in view of Campbell (U.S. 4,605,820)

In referring to claim 24:

Limitation "the device as set forth in claim 23, further comprising a second logic, the second logic using the generation keys and the device identification to generate the at least one key" is matched (column2, lines 38-47; column 3, lines 45-67; column 4, lines 1-6, 41-44). Tatu Ylonen disclosed

-At least one first device, said first device comprising:

- A non-volatile storage medium for storing information for at least one key corresponding to a device identification of first device
- A first logic to encode data using the at least one key and decode encoded data using the at least one key
- An input/output to communicate encoded data in a message, the message including the device identification of the first device and the encoded data

-At least on second device coupled to the first device through the communication medium, the second device comprising:

- A non-volatile storage medium for storing information for at least one key corresponding to a device identification of the first device.
- A second logic to encode data using the at least one key and decode encoded data using the at least one key.
- An input/output to communicate encoded data in a message, the messages including the device identification of the first device and the encoded data.

But he failed to teach this limitation: "the device as set forth in claim 23, further comprising a second logic, the second logic using the generation keys and the device identification to generate the at least one key." However, Campbell disclosed key management system for on-line communication. Campbell taught how to generate the 50 values what are equivalent to the "generation keys" of primary key table by using one first initial double-length key what is equivalent to "device identification" proceeds with elements in the modifier table. In Campbel's method, After 10 entries of the first column of primary key table have been generated by using the first initial double-length key, the next step is generation 10 entries for the second column of primary key table by using the every first entry of the first column as the input value proceeds with the elements in the modifier table. For the third column, using the every first entry of second column to generate 10 entries in third column. This procedure continues until all row of all five columns have been generated. It would have been obvious to a person of ordinary skill in the art at the time the invention was make of "the device as set forth in claim 23, further comprising a second logic, the second logic using the generation keys and the device identification to generate the at least one key." because first entries of each column what

have been used as the input values to generate next 10 entries in the next column are "generation keys", the hex digits of each input entry what is used for generation 10 entries of next is also device identification. So, Ideally Campbell's method meets limitation of "the device as set forth in claim 23, further comprising a second logic, the second logic using the generation keys and the device identification to generate the at least one key." The motivation would have been obvious because on of ordinary skill in the art would have been motivated to improve security key system for on-line communication and there is no need for large storage of keys at the central host.

Conclusion

~~The prior art made of record and not relied upon is considered pertinent to applicant's disclosure, as the prior art teaches or suggests~~

~~US Patents:~~

Any inquiry concerning this communication or earlier communications from the examiner should be directed to lan dai thi truong whose telephone number is 571-272-7959. The examiner can normally be reached on monday- friday from 8:30am to 5:00 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Lan Dai Thi Truong
Examiner
Art Unit 2132

Ldt
11/30/2004

GILBERTO BARRON SR
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100